学校编码：10384　　分类号＿＿密级＿＿
学　　号：23320071152176　　UDC＿＿

硕　士　学　位　论　文

EAP-AKA 认证协议的研究和实现

Research and Implement of EAP-AKA Authentication Protocol

宋志贤

指导教师姓名：肖明波　　教授
专　业　名　称：通信与信息系统
论文提交日期：2010　年　5　月
论文答辩时间：2010　年　5　月
学位授予日期：2010　年　　月

答辩委员会主席：＿＿＿＿＿＿
评　　阅　　人：＿＿＿＿＿＿

2010　年　5　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

无线局域网(WLAN)以其使用灵活、部署简单、费用便宜等优点得到广泛的使用，成为有线网络的很好的延伸和补充。3G 网络是最大的通信网络之一，它提供全球漫游和良好的安全机制。3G 与 WLAN 融合可以实现优势互补，既保留 3G 在计费管理、漫游和安全方面的优势，又能以较低的成本实现热点覆盖。异构网络之间的互连互通使得安全性变得更加重要。

可扩展认证协议(EAP)是 WLAN 认证架构的核心部分。EAP 认证包括 EAP-TLS 和 EAP-AKA 等方式。EAP-TLS 是重要的 EAP 方法，可以提供双向身份认证和密钥分发。EAP-AKA(Extensible Authentication Protocol-Authentication and Key Agreement，扩展认证协议-认证与密钥协商)是 3G 与 WLAN 互连的认证和密钥分配协议，是一种基于 3G 的认证与密钥协商(AKA)机制的 EAP 方法。在不修改 3G 安全体系的基础上，EAP-AKA 认证实现互连网络中用户的身份认证和密钥分配。

论文分析 3G 和 WLAN 互连结构的安全方案，分析 EAP 的两种重要方法：EAP-TLS 和 EAP-AKA。论文先实现基于 RADIUS 的 EAP-TLS 证书认证网络。接着论文重点介绍 EAP-AKA 认证方法，分析 EAP-AKA 的用户名管理机制、具体报文格式、完全认证模式以及快速重认证模式。论文描述 EAP-AKA 认证网路各个模块的功能以及 EAP-AKA 服务器的状态机。通过在 freeradius 服务器中添加 AKA 认证方式，实现 EAP-AKA 服务端功能。通过对 EAP-AKA 认证缺陷的分析，论文提出一种结合 EAP-TLS 和 EAP-AKA 的改进方案，并给出改进方案的实施条件和步骤。该方案能对认证者进行认证和保护密钥材料的传输。最后，论文给出配置 3G 智能卡的用户终端在 3G-WLAN 互连网络的认证场景，即用户既可以通过 AKA 认证由 3G 网络接入，也可以通过 EAP-AKA 认证由 WLAN 接入。

关键词：EAP-AKA；3G 网络；无线局域网

Abstract

Wireless Local Area Network has been booming in the last few years, due to it's being a very flexible data communication system and a low cost network. WLAN makes up the LAN. The 3G network is one of the biggest communication networks being applied now and in the future. 3G networks supply global roaming and robust security. 3G-WLAN integrating networks may take advantage of both the low cost of WLAN, and 3G's security mechanism. The security issues become more important in the interconnection of heterogeneous networks.

EAP is the core of WLAN authentication architecture.EAP methods includes EAP-TLS, EAP-AKA and etc. As an important EAP method, EAP-TLS carries out ID verification and key distribution. EAP-AKA method is the Authentication and key distribution protocol of 3G-WLAN integrating networks. It's base on the 3rd generation Authentication and Key Agree protocol (AKA). EAP-AKA supplies ID verification and key distribution without any change of the 3G security mechanism.

We analyze the security architecture of 3G-WLAN integrating networks in the dissertation and mainly include two important EAP methods: EAP-TLS and EAP-AKA. First, we analyse EAP-TLS (Transport Layer Security) certificate verification networks and carry it out base on RADIUS. Then, we give detailed explanations of the EAP-AKA method, analyze its username management mechanism, full and fast reauthentication mode and then give the concrete format of the messages. After that we show the functions of EAP-AKA authentication network entities and the state machine of EAP-AKA server. Then we develope the EAP-AKA scheme using open source sofeware freeradius, and test the developed EAP-AKA method. The debug result shows that EAP-AKA method developed can perform effectivelly.

Also, we make some improvements inlight of its security defects, and

show how to carry it out. The improved method demands that AAA server should carry out EAP-TLS Authentication with AP before EAP-AKA. The AP can be verified and key information can be transmitted confidentially. Finally，we demonstrate the 3G-WLAN integrating network authentication scenario: a user device equipped 3G USIM can use the EAP-AKA for authentication through WLAN or use the AKA for authentication via 3G to access the 3G-WLAN integrating network.

Keywords：EAP-AKA；3G；WLAN

目录

Contents

第一章 绪论

1.1研究背景

如今无线通信技术正以前所未有的速度发展，迅速并广泛地融入人们的生活中。无线局域网具有移动性好、建网迅速、速率高、便捷等特点，作为无线接入的有效手段，WLAN 在近年来得到飞快的发展。蜂窝移动通信网技术比较成熟，网络覆盖能力强。特别是 3G 网络，能够提供广域覆盖和全球漫游。

通信的理想目标就是要实现“5W”信息通信，即任何人可在任何时候、任何地方、与任何人进行任何种类的通信。未来多种异构接入和网络的并存，网络融合和终端融合是必然的趋势。3G 网络与 WLAN 互连网络，既能发挥 3G 网络的更高的移动速度、广泛覆盖和充分的安全措施的优势，同时又能发挥 WLAN 较低的成本提供远高于 3G 的数据传输速率。因此，WLAN 可以作为 3G 网络的有效补充而存在。

随着数据业务的增多，网络的安全问题日益受到关注。如何对用户实施有效的认证、授权和计费功能成为一个急待解决的问题。3GPP 要求 3G 和 WLAN 网络融合建立在不修改 3G 安全体系的基础上，因此融合网络的认证和密钥分配基于 3G 的认证和密钥协商 AKA 过程。3G AKA 的质询/应答机制独立于网络并可在其他传输机制中运行。802.11i 中定义可扩展认证协议/用户识别卡(EAP/SIM)、EAP-AKA 认证技术使得 WLAN 与 GSM 网络以及 3G 网络能够互通。

1.2研究内容

本文对 WLAN 和 3G 互连网络的安全结构进行分析，阐述相关的 AAA (Authentication Authorization Accout，认证、授权、计费)协议，EAP 协议，对 EAP-AKA 认证方式进行详细的分析，实现 EAP-TLS 证书认证网络，并在 freeradius 下添加 EAP-AKA 认证方式。论文主要研究的内

容：

（1） WLAN 和 3G 互连安全结构

本文介绍 3G 网络和 WLAN 的安全现状。3G 网络和 WLAN 互连可以优势互补，但是互连网络的安全问题更为复杂。论文研究 3G 和 WLAN 互连结构的安全方案。

（2） EAP-TLS 证书认证网络

EAP-TLS 证书认证实现密钥交换和身份认证。论文实现 EAP-TLS 证书认证网络，实现证书认证接入网络。

（3） EAP-AKA 认证的研究和实现

802.11i 中定义 EAP-AKA 认证技术使得 WLAN 与 3G 网络能够互通。论文深入分析 EAP 协议、EAP-AKA 认证方式。

在 freeradius 下添加 EAP-AKA 认证方式，测试并分析认证调试结果。通过调试结果的分析，验证添加的 EAP-AKA 方式的可用性。论文分析 EAP-AKA 认证的缺陷，并提出改进方案，给出改进方案的实施条件和步骤。

（4） 3G 和 WLAN 互连网络中 EAP-AKA 的实现

装备 3G 运营者发行的 USIM(Universal Subscriber Identity Module，通用用户模块)卡的用户设备可以通过 3G 网络直接进行 AKA 认证接入，也可以通过 WLAN 网络进行 EAP-AKA 认证接入互连网络。后端的服务器协议可以采用 RADIUS(Rmote Athentication Dal-in Srvice，远程接入用户认证服务)或者 Diameter 协议。

1.3 论文组织结构

第一章为绪论，本章主要介绍 WLAN 与 3G 网络的发展和安全现状，以及 3G 和 WLAN 互连的必然趋势。同时介绍论文中主要研究的内容，以及论文的组织结构。

第二章介绍 WLAN 安全现状，3G 的安全保护，以及 3G 和 WLAN 互连的安全结构。着重分析 EAP 协议，比较几种常见 EAP 方法，并分析 EAP-AKA 的安全性。

第三章分析 EAP-TLS 证书认证体系，配置 freeradius 服务器，生成数字证书，配置证书网络，实现证书认证接入。

第四章重点介绍 EAP-AKA 认证方法，分析 EAP-AKA 的用户名管理机制、具体报文格式、完全认证模式以及快速重认证模式。接着描述 EAP-AKA 认证网路各个模块的功能以及 EAP-AKA 服务器的状态机。通过在 freeradius 服务器中添加 AKA 认证方式，实现 EAP-AKA 服务端功能。通过对 EAP-AKA 认证缺陷的分析，论文提出一种结合 EAP-TLS 和 EAP-AKA 的改进方案，并给出改进方案的实施条件和步骤。

第五章系统分析 3G 和 WLAN 互连的安全认证过程，给出配置 3G 智能卡的用户终端在 3G-WLAN 互连网络的认证场景。

最后一章给出总结和展望。首先总结论文所作的工作。同时由于现有条件的局限性，对未来的 3G-WLAN 互连安全工作做进一步展望。

第二章 WLAN 和 3G 互连的安全认证

2.1WLAN 和 3G 的互连安全

2.1.1 3G 网络安全

（1） 3G 网络介绍

随着 GSM 在全球的成功以及通信技术的发展，移动通信系统已经走到第三代(3G)通信时代。国际电信联盟(ITU)在全球范围内征集第三代通信(IMT-2000)无线传输技术(RTT)提案，以期获得统一的标准。对于采用频分双工(FDD)和时分双工(TDD)的 IMT-2000 移动通信系统，数据传输能力要求标准[1]：(1)高速移动环境(FDD：500km/h，TDD:120km/h):144Kbps；(2)室内或室外，手持机环境(30km/h)：384Kbps；(3)室内环境(3km/h)：2Mbps。1999 年底召开的 ITU TG8/1 最后一次会议上，通过包括 TD-SCDMA ,WCDMA,CDMA2000 等三种制式作为 IMT-2000 的无线接口技术规范标准。2007 年，无线宽带技术 WiMax 也正式成为 3G 标准。

（2） 3G 网络安全

3G 不仅提供语音业务,也提供各种数据和多媒体业务.一些数据业务,如移动电子商务和网上银行,对未来网络的安全性有更高的要求.如果缺乏足够的安全性,3G 系统的很多网络服务,新型业务都将难以真正使用.第三代通信提出如下的安全目标[2]:

1. 用户信息不被窃听或盗用
2. 网络提供的资源信息不被滥用或盗用
3. 安全特征应该充分标准化-保证至少有一个算法符合全球标准化
4. 安全级别高于目前移动网和固定网的安全等级
5. 安全特征具有可扩展性

3G 的安全网络结构如下:

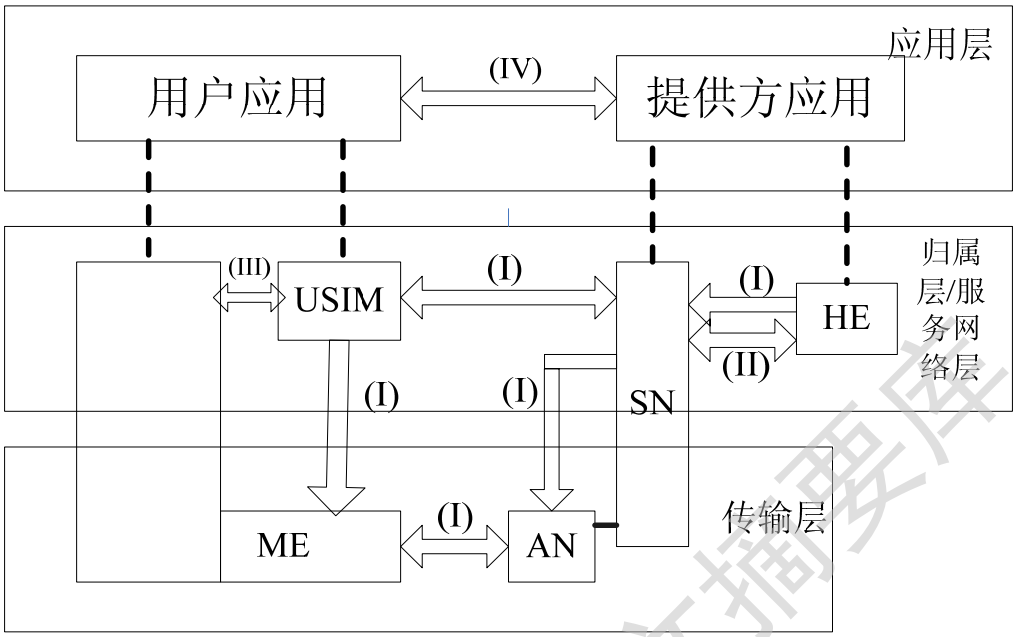

图 2-1 3G 安全架构

3G 的总体安全网络结构可以分为 5 个层面 5 个部分：

网络接入安全(I)：该安全特征集提供安全接入 3G 服务网的机制，抵御对无线链路的攻击。其功能包括：用户身份保密，认证和密钥分配，数据加密和完整性等。其实认证和密钥分配是基于 USIM 和 HE/AuC 共享密钥信息的相互认证，其中融合加密，完整性保护等措施；

网络域安全(II)：该安全特征集使在服务域中的结点能够安全地交换信令数据，抗击在有线网络上的攻击；

用户域安全(III)：该安全特征集保证对移动台的安全接入，包括用户与智能卡之间的认证，智能卡与终端间的认证及其链路的保护；

应用域安全(IV)：该安全特征集是用户域与服务提供商的应用程序间能安全的交换信息；

安全的可视性和可配置型(V)：该安全域主要使用户能获知一个安全特征集是否在运行，以及服务提供商提供的服务是否依赖该安全特征。

网络元素在安全结构中扮演的角色以及各实体更清晰的关系如下：

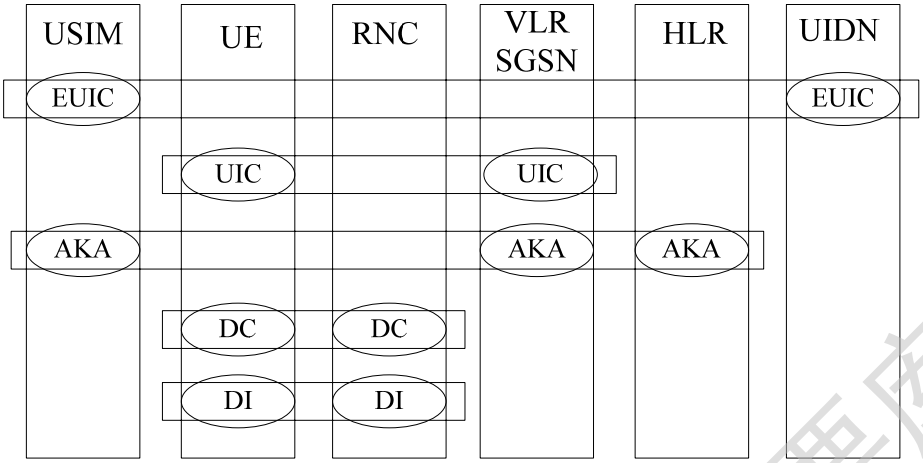

图 2-2 3G 安全功能结构

1. 纵向代表网络元素：

--用户域：USIM 和 UE

--在服务网络(SN)域：RNC 和 VLR，SGSN

--在归属环境(HE)域：HLR/AuC 和 UIDN

2. 横向代表安全机制

--EUIC:增强用户身份保密机制(可选，位于用户和 HE 之间)

--UIC:用户身份保密性的常规机制(位于用户和服务网络之间)

--AKA:认证和密钥协商机制，包括用户触发重认证功能，即控制接入密钥的生命周期

--DC:用户数据和信令数据的保密性机制

--DI:信令数据的完整性机制

--DEC:网络范围内的数据保密性机制

（3） 3G 系统中的安全算法

3G 的安全功能主要分四类：认证与密钥协商(AKA)，消息数据保密(DC),完整性保护(DI)和用户身份保密(UIC)。AKA 协议中的算法 f_1,f_2,f_3,f_4,f_5 和 UIC 中的算法 f_6 和 f_7 无需进行标准化，可由运营商或制造商自行确定，而无线链路的保密性和完整性算法即 f_8 和 f_9 的核心算法采用标准化，并为算法设定一个 4bits 的标识号。

AKA 中参与认证和密钥协商的主体有三个：用户终端(ME/USIM)，